ABSTRACT

AES MIXCOLUMN TRANSFORM

A simplified logic circuit for performing the AES Rijndael MixColumns transform exploits the common relationship between each of the successive rows of the transform matrix and its preceding row. A logic circuit for performing multiplication of an (m × n) matrix by a (1 × n) or by a (m × 1) matrix, where m is a number of rows and n is a number of columns, and where each successive row, m, of n elements is a predetermined row permutation of a preceding row comprises: n multiplication circuits; n logic circuits; n registers for receiving logical output from the logic circuits; feedback logic for routing the contents of each register to a selected one of inputs of the logic circuits in accordance with a feedback plan that corresponds to the common relationship between successive matrix rows; and control means for successively providing as input to each of the n multiplication circuits each element in the (1 × n) or (m × 1) matrix.

(Figure 2)